UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/885,959 | 06/22/2001 | Robert Gallant | 06944.0037 | 6201 |

27871 7590 06/22/2005

BLAKE, CASSELS & GRAYDON LLP
BOX 25, COMMERCE COURT WEST
199 BAY STREET, SUITE 2800
TORONTO, ON M5L 1A9
CANADA

| EXAMINER | |
|---|---|
| LANIER, BENJAMIN E | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2132 | |

DATE MAILED: 06/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/885,959 | GALLANT ET AL. | |
| | Examiner | Art Unit | |
| | Benjamin E Lanier | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *30 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Amendment*

1. Applicant's amendment filed 19 May 2005 amends claims 1, 8-10, 17, 18. Applicant's amendment has been fully considered and is entered.

### *Response to Arguments*

2. Applicant's arguments filed 19 May 2005 have been fully considered but they are not persuasive. Applicant's argument that Mullin does not teach how to compute a scalar multiple of a point is not persuasive because Applicant admits on Page 5 of their remarks that Mullin discloses how to derive the scalar multiple of a new point.

3. Applicant's argument that Mullin does not disclose performing a scalar multiplication on a point is not persuasive because Mullin discloses multiplying any point on a curve by an integer k to produce a further point on the curve (Col. 2, lines 27-29).

4. With respect to the provisional Double Patenting rejection in view of co-pending Application No. 09/031,013, the rejection will maintained because as of 20 June 2005 Application No. 09/031,013 has not been abandoned.

### *Double Patenting*

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. Claims 1-12, 14-18 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-16 of copending Application No. 09931013. Although the conflicting claims are not identical, they are not patentably distinct from each other because application claims a method for multiplying an elliptic curve point Q by selecting an elliptic curve over a finite field F, establishing a representation of said scalar k as a combination of components ki and an integer, combining said representation and said point Q to form a composite representation of a multiple corresponding to kQ, and computing a value corresponding to said point kQ from said composite representation of kQ.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an

international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

8. Claims 1-7, 10-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Mullin, U.S. Patent No. 5,999,626. Referring to claims 1, 5, 6, 10, 14, 16, Mullin discloses a frobenius operator (Ø) being applied to an elliptic curve, to generate key pairs, at least one of the coordinates representing a point in the initial set to provide a coordinate of a further point on the elliptic curve. For a curve over a finite field, there are m frobenius operators so for each value of kP stored in the initial set, m values of kP may be generated, referred to as derived values. The new value of k associated with each point can be derived from the initial relationship between P and ØP and the initial value of k (Col. 3, lines 47-60). The frobenius operator Ø operates on a point P having coordinates (x,y) on an anomalous elliptic curve in a finite field such that $Ø^1P = (x^2,y^2)$. Moreover, the point $Ø^1P$ is also on the curve. For each value of $Ø^1(kP)$, it is necessary to obtain the corresponding value of $kØ(P) = \dot{\lambda}P$. $\Lambda$ is a constant that may be evaluated ahead of time and the values of its first m powers. It will be seen therefore that new session pairs k, kP may be derived simply and efficiently from the elements of the initial set. These session pairs may be computed in real time (Col. 6, lines 10-64). Mullin further teaches representation is of the form $ki = \Sigma\ ki\ \lambda \bmod n$ where n is the number of points on the elliptic curve (Col. 7, lines 3-6, 62-64).

Referring to claims 2, 11, Mullin teaches each of said components ki is shorter than said scalar k (Fig. 3).

Referring to claims 3, 12, 15, Mullin teaches components ki are initially selected and subsequently combined to provide said scalar k (Fig. 3).

Referring to claims 4, 13, Mullin discloses that the components are selected randomly (Col. 8, lines 11-15).

Referring to claims 7, 16, Mullin discloses the value of said multiple kQ is calculated using simultaneous multiple addition (Col. 10, lines 4-6).

***Claim Rejections - 35 USC § 103***

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

11. Claims 9, 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mullin, U.S. Patent No. 5,999,626, in view of Reiter, U.S. Patent No. 6,243,467. Referring to claims 9, 18, Mullin discloses a frobenius operator (Ø) being applied to an elliptic curve, to generate key pairs, at least one of the coordinates representing a point in the initial set to provide a coordinate of a further point on the elliptic curve. For a curve over a finite field, there are m frobenius operators

so for each value of kP stored in the initial set, m values of kP may be generated, referred to as derived values. The new value of k associated with each point can be derived from the initial relationship between P and ØP and the initial value of k (Col. 3, lines 47-60). The frobenius operator Ø operates on a point P having coordinates (x,y) on an anomalous elliptic curve in a finite field such that $Ø^1P = (x^2,y^2)$. Moreover, the point $Ø^1P$ is also on the curve. For each value of $Ø^1(kP)$, it is necessary to obtain the corresponding value of $kØ(P) = \lambda P$. $\Lambda$ is a constant that may be evaluated ahead of time and the values of its first m powers. It will be seen therefore that new session pairs k, kP may be derived simply and efficiently from the elements of the initial set. These session pairs may be computed in real time (Col. 6, lines 10-64). Mullin further teaches representation is of the form $ki = \Sigma\ ki\ \lambda \bmod n$ where n is the number of points on the elliptic curve (Col. 7, lines 3-6, 62-64). Mullin does disclose obtaining fractions f0 f1 representative of the vector v, applying said fractions to k to obtain a vector z, calculating an efficient equivalent v' to the vector v and using components of the vector v' in the composite representation of kQ. Reiter teaches components ki are obtained by obtained short basis vectors (U0, U1) of the field F, designating a vector v as (k, O), converting v from a standard, orthogonal basis to the (U0, U1) basis (Col. 6, lines 24-36). Reiter further discloses an extended Euclidean algorithm to obtain fractions f0 f1 representative of the vector v, applying said fractions to k to obtain a vector x, calculating an efficient equivalent v' to the vector v and using components of the vector v' in the composite representation of kQ (Col. 2, lines 51-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Reiter with the system of Mullin in order to provide a method of encryption ultizing elliptic curves that is

computationally efficient and effective by reducing the base expansion in non-adjacent form as taught in Reiter (Col. 5, line 4 – Col. 6, line 14).

12. Claims 8, 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mullin, U.S. Patent No. 5,999,626, in view of Menezes. Referring to claims 8, 17, Mullin discloses a frobenius operator (Ø) being applied to an elliptic curve, to generate key pairs, at least one of the coordinates representing a point in the initial set to provide a coordinate of a further point on the elliptic curve. For a curve over a finite field, there are m frobenius operators so for each value of kP stored in the initial set, m values of kP may be generated, referred to as derived values. The new value of k associated with each point can be derived from the initial relationship between P and ØP and the initial value of k (Col. 3, lines 47-60). The frobenius operator Ø operates on a point P having coordinates (x,y) on an anomalous elliptic curve in a finite field such that $Ø^1P = (x^2,y^2)$. Moreover, the point $Ø^1P$ is also on the curve. For each value of $Ø^1(kP)$, it is necessary to obtain the corresponding value of $kØ(P) = \lambda P$. $\Lambda$ is a constant that may be evaluated ahead of time and the values of its first m powers. It will be seen therefore that new session pairs k, kP may be derived simply and efficiently from the elements of the initial set. These session pairs may be computed in real time (Col. 6, lines 10-64). Mullin further teaches representation is of the form $ki = \Sigma\ ki\ \lambda \bmod n$ where n is the number of points on the elliptic curve (Col. 7, lines 3-6, 62-64). Mullin does not disclose grouped terms Gi utilized in a simultaneous multiple addition. Menezes discloses grouped terms Gi utilized in a simultaneous multiple addition (Page 618), which meets the limitation because Gi is defined and simultaneous multiple addition is analogous to simultaneous multiple exponentiation as taught by Menezes. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the

teachings of Menezes with the system of Mullin because Menezes teaches an efficient method for multiplying two elements in the Group G to perform efficient exponentiation (Pages 613-614).

***Conclusion***

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100